WinExec

Vulnerable to white space issues in executable or path name. Applications should use the CreateProcess function.

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4726 bytes

Attack Category	Path spoofir	Path spoofing or confusion problem		
Vulnerability Category	Process man	Process management		
Software Context	Process Man	Process Management		
Location	• winbase.h	• winbase.h		
Description	The WinExec fur	The WinExec function runs the specified application.		
	This function is provided only for compatibility with 16-bit versions of Windows. Applications should use the CreateProcess function.			
	space-delimited sexecutable or patrisk that a difference	The executable name is treated as the first white space-delimited string in lpCmdLine. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces.		
APIs	Function Name	Cor	nments	
	WinExec			
Method of Attack	called "Program." incorrectly calls of directory will not intended applicate MSDN article, Application Secundary Implications of Computer of Comput	"If a malicious user were to create a Trojan program called "Program.exe" on a system, any program that incorrectly calls WinExec using the Program Files directory will now launch the Trojan instead of the intended application." - MSDN article, "A Great Step Forward in Application Security: Documenting Security Implications of C Runtime and Windows APIs" by Michael howard http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp>		
Exception Criteria				
Solutions	Solution Applicability	Solution Description	Solution Efficacy	
	When desiring to run a	Use CreateProces function.	Effective.	

^{1.} http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

WinExec 1

Discriminant Set	Operating Syste	• W	indows	
Recommended Resource				
Source References	 http://msdn.microsoft.com/library/default.asp? url=/library/en-us/dnsecure/html/appsec.asp² http://msdn.microsoft.com/library/default.asp? url=/library/en-us/dllproc/base/winexec.asp³ 			
	WinExec("\"C:\\Program Files\ \MyApp.exe\" -L -S",)			
Examples of Corrected Code	To avoid this problem, use CreateProcess rather than WinExec. However, if you must use WinExec for legacy reasons, make sure the application name is enclosed in quotation marks as shown in the example below.			
	The executable name is treated as the first white space-delimited string in lpCmdLine. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces.			
	If a malicious user were to create an application called "Program.exe" on a system, any program that incorrectly calls WinExec using the Program Files directory will run this application instead of the intended application.			
Examples of Incorrect Code		<pre>WinExec("C:\\Program Files\ \MyApp",)</pre>		
Signature Details	_	LPCSTR lpCmdLine, UINT uCmdShow		
	application If you must use WinExec for legacy reasons	Make sure the application name is a fully qualified path and wrap each command line element with double quotes.	Effective.	
	specified			

Languages	•	С
	•	C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

WinExec 3

^{1.} mailto:copyright@cigital.com